Annual Privacy Training

Note, DSCA modified this training module from the original version created by OSD/JS Privacy Office.

Training Requirements

- This training is required under DoD 5400.11-R, DoD Privacy Program.

- All civilian and military employees are required to complete this training. DoD Contractor employees with access to a government computer or a DoD system of records must also complete this training.

- In order to receive credit for completing this training module, employees must complete the "***Automated Proof of Training***" slide provided at the end of this slide to ensure the Office of General Counsel receives the self-generating email notification.

Main Points

The main points that will be covered in this training module are as follows:

- Statutory/Regulatory Authorities
- Purpose of the Privacy Act
- Policy Objectives
- Definitions
- System of Record Notice (SORN)
- Privacy Act Statement
- DoD SSN Reduction Program
- Disclosure
- Accessing Records
- Safeguarding Personally Identifiable Information (PII)
- Criminal and Civil Penalties
- Privacy Breach
- Your Role and Responsibility
- Contact Information

Statutory/Regulatory Authorities

Statutory Authority:
The Privacy Act of 1974, as amended (5 U.S.C. 552a), as implemented by OMB Circular No. A-130

DoD Regulatory Authorities:
- DoD Directive 5400.11
- DoD Regulation 5400.11-R
- OSD Administrative Instruction No. 81

Purpose of the Privacy Act

The Privacy Act of 1974 is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them.

Policy Objectives

The Act focuses on four basic policy objectives:

1)To restrict disclosure of personally identifiable records maintained by agencies.

2)To grant individuals increased rights of access to agency records maintained on themselves.

3)To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.

4)To establish a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

Definitions

Agency: "any Executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the [federal] Government (including the Executive Office of the President), or any independent regulatory agency." 5 U.S.C. § 552a(1) (incorporating 5 U.S.C. § 552(f) (2006), which in turn incorporates 5 U.S.C. § 551(1) (2006)).

Individual: "a citizen of the United States or an alien lawfully admitted for permanent residence." 5 U.S.C. § 552a(a)(2).

Note, non-U.S. citizens are not covered by the Privacy Act. However, agencies must ensure the country's privacy / data protection legal requirements are met. In addition, the Privacy Act does not cover deceased persons, but the release of information is protected when the release would invade the privacy of the surviving next of kin.

Definitions (*continued*)

Record: "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4).

System of Records: "a group of any records under the control of any agency from which information is **retrieved** by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5).

System of Record Notice (SORN)

The Privacy Act requires Federal agencies to publish a notice for public comment in the Federal Register which describes, among other things, the existence, uses, and legal authority for the collection of each new or significantly revised system of records.

When an agency maintains information about an individual and retrieves that information by the individual's unique personal identifier such as a name or tracking number, a Privacy Act System of Records exists, and a SORN is **required**.

Examples of a "system of records" may include the following:

- IT systems funded by DSCA for data management, including systems maintained in a commercial environment;
- Applications such as Microsoft Access or Excel used to create databases or spreadsheets; and
- Paper or physical records maintained in file cabinets or drawers.

DoD Privacy Program regulation states, "the system notice must be published in the Federal Register **before a Component begins to operate** a system (e.g., collect or use the information).

SORN (continued)_

A SORN is a blueprint as it provides the following information to the public about your data collection:

- *System identifier*
- *System name*
- *System location*
- *Categories of individuals covered by the system*
- *Categories of records in the system*
- *Authority for maintenance of the system*
- *Routine uses of records maintained in the system*
- *Disclosure to consumer reporting agencies: (Entry is optional)*
- *Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system for the system*
- *Storage:*
- *Retrievability*
- *Safeguards*
- *Retention and disposal*
- *System manager(s) and address*
- *Notification procedure*
- *Record access procedures*
- *Contesting record procedures*
- *Record source categories*
- *Exemptions claimed for the system*

SORN (continued)

The SORN is the foundation of Privacy programs.

- It's transparency - enables the public to know what data is being collected and on whom.
- It's federal rulemaking – published in Federal Register.
- It's a medium to answer privacy related questions.
- It's the authority for sharing information with others.
- It's the blueprint that describes your business practices.
- It's something that we review and update biennially to reflect changes in business practices.

Privacy Act Statement

When an agency solicits personal information from an individual for a system of records, the Privacy Act requires agencies to tell the individual in writing of:

- *Authority*: The statute or executive order of the President that authorizes the agency to solicit the information.
- *Purpose*: The principal purposes for which the information is intended to be used.
- *Routine Uses*: How the information will be used.
- *Disclosure*: Whether the disclosure of the information is mandatory or voluntary, and the effects, if any, on the individual for not providing all or any part of the information.

IMPORTANT NOTE

DoD SSN Reduction Program

DoDI 1000.30, "Reduction of Social Security Number (SSN) Use Within DoD," August 1, 2012, requires Components to eliminate all unnecessary collections of SSNs. Components are permitted to use SSNs if such use is authorized by law, required for interoperability with organizations outside DoD, or required due to operational necessities. DoDI 1000.30, para 2(c) describes 13 general categories of acceptable uses:

1)Geneva Conventions Serial Number ***(DoD Identification Number will replace the SSN as the Geneva Conventions Serial Number for the United States as all DoD identification cards are updated)***
2)Law Enforcement, National Security and Credentialing
3)Security Clearance Investigation and Verification
4)Interactions with Financial Institutions
5)Confirmation of Employment Eligibility
6)Administration of Federal Worker's Compensation
7)Federal Taxpayer Identification Number
8)Computer Matching ***(This use category pertains to the Computer Matching and Privacy Protection Act of 1988 which involves the sharing of personal information among Federal agencies, including State and Local agencies, for purposes of establishing or verifying eligibility for Federal benefit programs or recouping payments or delinquent debts.)***
9)Foreign Travel
10)Noncombatant Evacuation Operations (NEOs)
11)Legacy System Interface
12)Operational Necessity

IMPORTANT NOTE

DoD SSN Reduction Program (*continued*)

13) Other Cases: (*According to DoDI 1000.30, the previous categories may not include all uses of the SSN authorized by law. However, should an application owner be able to show sufficient grounds that a use case not specified above is required by law, may continue to use the SSN. However, a application owner who seeks to use this use case as justification must provide specific documentation in order to continue to use the SSN in accordance with this provision.*)

Disclosure

No agency shall disclose any record which is contained in a system of records by any means of communication to any person or another agency without a written request or prior consent of the individual to whom the record pertains unless the disclosure of the record would be to those officers and employees of the agency who have a need for the records in performance of their duty or for an established routine use to another Federal agency.

The Defense Privacy and Civil Liberties (DPCLO) publishes a list of DoD blanket routine uses on its website:

http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx

Accessing Records

The individual about whom the record pertains is usually entitled to access his or her own record. The Privacy Act SORN for the pertinent records provides the address one may use to request access to his or her records.

If the individual believes factual information contained in their record is in error, he or she should follow procedures identified in the system notice for requesting correction of the record. If the system manager refuses to make corrections requested by the individual, the individual may continue to pursue correcting his or her record through the appeal process.

Safeguarding Personally Identifiable Information (PII)

PII is any information that can be used to distinguish or trace a person's identity. See DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007, for the official definition of PII.

There are differences in PII as the degree of its sensitivity varies. For example, the sensitivity of a name and an address is less than a name and a SSN. Note, PII with a higher degree of sensitivity requires stricter handling guidelines because of the increased risk to an individual if compromised.

Some categories of PII are sensitive as stand-alone data elements: Examples include:

- Social Security number
- Driver's license, passport and other identification numbers;
- Financial Account Number
- Biometric Identifier

Safeguarding PII (*continued*)

However, data elements when paired with another identifier such as a name are also considered sensitive PII. Examples include but not limited to:

- Citizenship
- Last 4 digits of SSN
- Date of Birth
- Medical Information
- Military Records
- Religious preference
- Home address and telephone number
- Law Enforcement Information
- Financial Information
- Race/Ethnicity
- Security Clearance
- Disability Information
- Child Information
- Place of Birth

Safeguarding PII (*continued*)

The Privacy Act requires agencies to:
- Establish Safeguards
- Maintain accurate, relevant, timely and complete records

Types of Safeguards:
- Physical
- Technical
- Administrative

IT system designers, system/program managers, and Component Privacy Officials are responsible for establishing safeguards.

PII must always be treated as “FOR OFFICIAL USE ONLY” and must be marked accordingly. This applies not only to conventional records but also to electronic (including email) transmissions and faxes, which must contain the cautionary marking “For Official Use Only – Privacy Act of 1974”; or “FOUO – Privacy Act Data” before the beginning of text containing Privacy Act information.

Safeguarding PII (*continued*)

***Physical*:**

- Paper records should be stored in cabinets
- Records being faxed mailed should have a Privacy Act Data Cover Sheet (DD Form 2923)
- Facilities handling PII should be access controlled and hardware should be locked up
- Never leave files, storage media, or computers unattended or in vehicles
- Use filtering devices on computer screens
- Records Disposal – retirement or deletion of a records does not remove the need for safeguards:
  - Must render discarded records unrecognizable and beyond reconstruction
  - Destruction should be appropriate to the type of media involved (e.g., paper: burn or shred; electronic: overwrite, degauss, or incinerate)

Safeguarding PII (*continued*)

***Technical*:**

- Encryption: Ensure all emails with PII are encrypted and the recipients have a "need to know" to perform official assigned duties.
- Remote Secure Access to DoD servers
- Ensure records are access controlled.
  - PII on shared drives should only be accessible to those with a "need to know."
- Timeout Function
- Log and Verify
- Ensure Understanding of Responsibilities
- Use Data Loss Protection Tools and PII Blocking

Overview of the Privacy Act of 1974

Safeguarding PII (*continued*)

***Administrative*:**

- Have polices in place for PII handling, specifically defining:
  - Affected Individuals
  - Affected Actions
  - Consequences

- Ensure staff handling PII are adequately trained:
  - Commensurate with responsibilities
  - Prerequisite before permitted access to DoD systems
  - Mandatory training for affected DoD personnel and contractors

Safeguarding PII (*continued*)

***Administrative*:**

It's is DoD policy that:

- All automated systems containing PII are registered in the Defense Information Technology Portfolio Repository (DITPR)

- Updates to OMB be designed so that:
  - IT systems with PII are reviewed on same cycle as Defense Information Assurance Certification and Accreditation Process (DIACAP)

(In March, 2014, DoD has officially begun its transition from the legacy DIACAP process to the new "Risk Management Framework (RMF) for DoD IT." See DoDI 8500.01, "Cybersecurity," March 14, 2014)

  - Privacy Impact Assessments (PIA) and SORNs reviewed at least once every two years
  - Results reported annually to DPCLO via the Federal Information System Management Act (FISMA) report

Safeguarding PII (*continued*)

Access to PII

- Protect PII at all times
- Do not share with anyone unless:
  - The SORN permits recipient access,
  - There is a "need to know" to perform official assigned duties, or
  - The subject of the record has provided written permission to disclose their information to the recipient
- Password protect PII placed on shared drives
- Monitor your actions to decrease the risk of unauthorized access

Remember:
You may be subject to criminal or civil penalties for violating the Privacy Act

Safeguarding PII (*continued*)

Teleworking with PII

- Paper records:
  - Place PII in locked drawers, locked briefcases, or other secure areas where family or household members, or unauthorized persons cannot access.

- Electronic records:
  - Use CAC access and password protection protocols
  - Do not share your CAC and password
  - Save, store and use PII only on DoD-issued equipment
  - Do not email work-related PII to your personal email account

For additional information regarding the handling of PII during telework, see DSCAI 1035.01, Telework Policy, August 19, 2015 and DD Form 2946.

Safeguarding PII (*continued*)

Transporting PII

- Follow the guidelines under DoD 5200.10, “DoD Information Security Program: Controlled Unclassified (CUI), February 24, 2012 (Volume 4)

- Hand carrying:
  - Use DD Form 2923, Privacy Act Data Cover Sheet to shield contents

- Ground Mail:
  - Double wrap envelope, if appropriate
  - Mark envelope to the attention of the “authorized” recipient
  - Never indicate on the outer envelope that the contents content PII

Safeguarding PII (*continued*)

Disposing PII

Use any means that prevents inadvertent compromise. A disposal method is considered adequate if it renders the information unrecognizable or beyond reconstruction.

Disposal methods may include:

- Burning
- Melting
- Chemical decomposition
- Pulping
- Pulverizing
- Shredding
- Mutilation
- Degaussing
- Empting a Computer's Recycle Bin after electronic file deletion

Criminal Penalties

- Any agency official or employee who willfully makes a disclosure of a record knowing it to be in violation of the Privacy Act or maintains a system of records without having published the requisite system notice may be convicted of a misdemeanor and fined up to $5000.

- Any person who knowingly and willfully requests or obtains a record of another individual from an agency under false pretenses may be convicted of a misdemeanor and fined up to $5000.

Civil Penalties

- *The Privacy Act also imposes civil penalties on violators who:*
  - Unlawfully refuse to amend a record.
  - Unlawfully refuse to grant access to records.
  - Fail to maintain accurate, relevant, timely and complete data.
  - Fail to comply with any Privacy Act provision or agency rule that results in an adverse effect.

- *Penalties include:*
  - Payment of actual damages
  - Payment of reasonable attorney's fees
  - Removal from employment

Privacy Breach

A breach is a loss of control, unauthorized disclosure, or unauthorized access of personal information when individuals other than authorized users gain access to such information an other than authorized purpose.

Upon becoming aware of the loss, theft, or improper disclosure of personal information (paper or electronic), you must report the incident to:

- Your Supervisor/Manager immediately;

- Electronic only: The United States Computer Emergency Readiness Team (US CERT) within one hour of discovery at https://forms.us-cert.gov/report/; and

- DSCA/OGC Privacy Officials within 24 hours at *dsca.ncr.ogc.mbx.pii-breach@mail.mil*. Note, your notice must contain information, required by Chapter 10.6.1.2. of DoD Directive 5400.11-R, "DoD Privacy

Your Role and Responsibility

- Do not collect PII without proper authorization.
- Do not maintain illegal files.
- Do not maintain or release inaccurate information.
- Do not distribute or release personal information to individuals who do not have a need for access.
- Do not maintain records longer than permitted.
- Do not destroy records before records retention requirements are met.
- Ensure that you do not place unauthorized documents in a records system.
- Ensure that you mark all documents that contain privacy information “For Official Use Only – Privacy Act of 1974”; or “FOUO – Privacy Act Data.”
- Ensure that all message traffic, faxes, and e-mails that contain personal information are properly marked and e-mail is encrypted.
- Think Privacy before you seek to establish new data collections on your computer or similar office equipment.

Contact Information

If you have any questions, please contact DSCA's Privacy Officials at dsca.ncr.ogc.list.ogc-all-members@mail.mil.

.

You completed your Annual Privacy Training Requirement!

To ensure you receive credit for meeting this annual requirement, click the link below to complete the automated email notification as well as obtain a copy of your certificate for your records.

(CLICK HERE)